

REMARKS

Applicants respectfully request reconsideration of the pending claims as follows.

The rejection of claim 25 as being unpatentable over Mochizuki (USP 7,020,780) in view of Sims (USP 6,550,011) and Shear (US Patent Publication No. 2001/0042043).

Applicant respectfully notes that the base reference Mochizuki is entirely inapposite as it teaches no encryption of the content by either the title key of the cipher key. Indeed, note what Mochizuki states in Col. 5, lines 55-64, where Mochizuki observes that the reproduction apparatus "is arranged [so] that it can reproduce a first scene of each software for example, however, it is impossible to reproduce succeeding scenes of the software unless a cipher key is produced." In other words, Mochizuki is using a specialized drive that refuses to read the "value-added" content unless the user produces a cipher key. It is just specialized hardware that is refusing to read content – i.e, this refusal is not based upon encryption but through hardware configuration of the drive. There is absolutely no discussion in Mochizuki with regard to any encryption or encryption algorithms.

Indeed, note what Mochizuki performs: in Col. 6, line 51, Mochizuki supposes he has a disk with a title key equaling "00666." This key and other information is sent to the software house, whereupon the software house returns a cipher key equaling "00421." (see Col. 7, line 8). As then discussed with regard to Mochizuki's Figure 4 in Col 7, lines 15-42, Mochizuki's host calculates another title key by combining the cipher key with additional information – in this case, he calculates "00666," which equals the original title key. Because this second title key equals the original title key, the user may then access the desired content. There is no decryption of encrypted content using any combination key whatsoever.

Note the stark differences between the Mochizuki scheme and what Applicants claim: we require that the disk contain "a locked file stored in mastered pre-recorded portion on a storage medium, the file being encrypted according to a content key and a complement key, the mastered pre-recorded portion including the content key but not the complement key, the storage medium also having an writeable area that is writeable by a engine." In other words, the disk must have mastered content that is encrypted according to a content key and a complement key. This is a much more secure method than the Mochizuki scheme – should a non-Mochizuki disk drive read a Mochizuki disk, the content is readily available because it is unencrypted. Even if one supposes that Mochizuki's content is encrypted according to the title key (for which there is no support or disclosure), the title key is on the disk so that a non-Mochizuki disk drive would still have access to the content.

It is thus incorrect to say that Mochizuki's title key is the analog to the claimed content key and that Mochizuki's cipher key is the analog to the claimed complement key: the cipher key in Mochizuki is used to do no decryption whatsoever – the cipher key merely represents a hashing of the title key such that upon an appropriate processing of the cipher key, the title key is returned. Never does Mochizuki decrypt any content using a combination of the title and cipher keys as required by the claims.

In sharp contrast, the method of claim 1 requires that the content be encrypted by both the content key and the complement key. Thus, if a locked disk is read by a hacker, that hacker only has access to the encrypted content and the content key and it thus unable to access (decrypt) the encrypted content.

But this fundamental flaw is not the only feature missing from Mochizuki: in addition, the claimed method requires the engine to write the complement key to the disk to unlock the locked content. This is quite advantageous with regard to a user's expectations: once a user has content on a disk, that user is accustomed to playing the content in multiple drives: for example, one might play a CD in the car and also the home. A user's expectations are violated if the CD plays only in the car but not in the home or vice versa. Here, the unlocked disk has both the content key and the complement key written to it so that a user may load the resulting unlocked disk into whatever drive he/she has available.

Thus, Mochizuki teaches no encryption nor does Mochizuki teach the writing of the unlock key (the complement key) to the disk.

The additional cited prior art does nothing to cure these fundamental flaws in Mochizuki. Applicant appreciates the citation of the Shears publication in that it does appear to disclose a drive which keeps its keys secret. However, that is not germane to the unlocking method being claimed: in other words, there is no suggestion or teaching from Shears so as to modify Mochizuki to provide the claimed method. Accordingly, claims 25 and 26 are in condition for allowance.

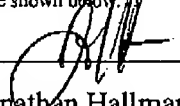
CONCLUSION

For the above reasons, pending Claims 25 and 26 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

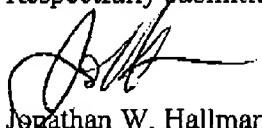
Certification of Facsimile Transmission

I hereby certify that this paper is being facsimile transmitted to (571) 273-8300 at the U.S. Patent and Trademark Office on the date shown below.

November 30, 2007


Jonathan Hallman

Respectfully submitted,


Jonathan W. Hallman
Attorney for Applicant(s)
Reg. No. 42,644